CLAIMS

1.   A secure document access method comprising:

capturing contents of a document;

generating a key from a cryptographic engine;

encrypting the contents of the document using said key by a multi-function

peripheral;

encoding the key;

storing said encrypted document;

communicating the encoded key to at least one authorized user; and

accessing the contents of the encrypted document utilizing said key by the at least

one authorized user.

2.   The method of claim 1, wherein the encoded key is transmitted to the at least one

authorized user in an electronic form.

3.   The method of claim 1, wherein the encoded key is represented by a half-tone

pattern.

4.   The method of claim 2, wherein the encoded key is output via a printer.

5.   The method of claim 2, wherein the encoded key is transferred to the at least one

authorized user in a secure manner.

6.   The method of claim 1, wherein the cryptographic key is generated via a software process.

7.   The method of claim 1, wherein the encryption specifies a maximum number of times the encrypted document is to be accessed.

8.   The method of claim 7, wherein a remaining number of times the document is available for output is indicated.

9.   The method of claim 1, wherein the encryption specifies a time by which the encrypted document is to be accessed.

10.   The method of claim 1, wherein a first multi-function peripheral captures the contents of the document and the authorized user accesses the document at a second multi-function peripheral.

11.   The method of claim 1, wherein said accessing of the encrypted document comprises the steps of:

    decoding said encoded key;

    locating the encrypted document;

    retrieving the encrypted document;

    decrypting the contents of the encrypted document; and

    outputting contents of the document.

Matter No. 200309942

12.   The method of claim 1, wherein contents of the document are captured line by line.

13.   A system for accessing a secure document comprising:

means for capturing contents of a document;

means for generating a cryptographic key;

means for encrypting contents of the document;

means for encoding said key;

means for storing the encrypted document;

means for communicating the encoded key to at least one authorized user; and

means for accessing the contents of the encrypted document utilizing said key by the at least one authorized user, wherein the contents of the encrypted document are encrypted by a multi-function peripheral.

14.   A multi-function peripheral comprising:

a scanner for capturing contents of a document;

a cryptographic engine for generating a cryptographic key;

at least one application specific integrated circuit (ASIC) programmed to encrypt contents of the document and to encode the cryptographic key;

a memory device for storing contents of the document; and

a facsimile device for transmitting data.

15.   The multi-function peripheral of claim 14 further comprising:

a digital sender unit for submitting the encoded key to a recipient in an electronic manner.

Matter No. 200309942

16.   The multi-function peripheral of claim 14 further comprising:

    a network card for communicating with another multi-function peripheral over a network.

17.   The multi-function peripheral of claim 16 wherein the network is a secure network.

18.   The multi-function peripheral of claim 14, wherein said cryptographic engine is another application specific integrated circuit (ASIC).

19.   The multi-function peripheral of claim 14, wherein said cryptographic engine is a software process.

20.   The multi-function peripheral of claim 14, wherein said at least one ASIC is programmed to decode the encoded key and to decrypt the encrypted document.

21.   The multi-function peripheral of claim 14 further comprising:

    a printer for outputting the key in the encoded form.

22.   The multi-function peripheral of claim 14, wherein the at least one ASIC is programmed to generate the cryptographic key.

23.   The multi-function peripheral of claim 14, wherein the facsimile machine transmits the key in the encoded form.

24. A machine readable medium comprising a computer program for causing a computer to:

create a document;

submit the document to a peripheral having a cryptographic engine; and

instruct the peripheral to encrypt contents of the document, said instructions further causing the peripheral to:

generate a key from the cryptographic engine;

encrypt contents of the document using said key;

store the encrypted document;

encode the key; and

transmit the key to at least one authorized user for accessing the encrypted document.